

NIST SP 800-53 with CNSSI 1253

Categorizing and Selecting Security Controls for National Security Systems



Connect. Integrate. Collaborate.

1-2 September 2009

Jennifer Fabius Greene

IC Certification and Accreditation Transformation Senior Risk Advisor

CREATE DECISION ADVANTAGE

Intelligence Community Chief Information Officer



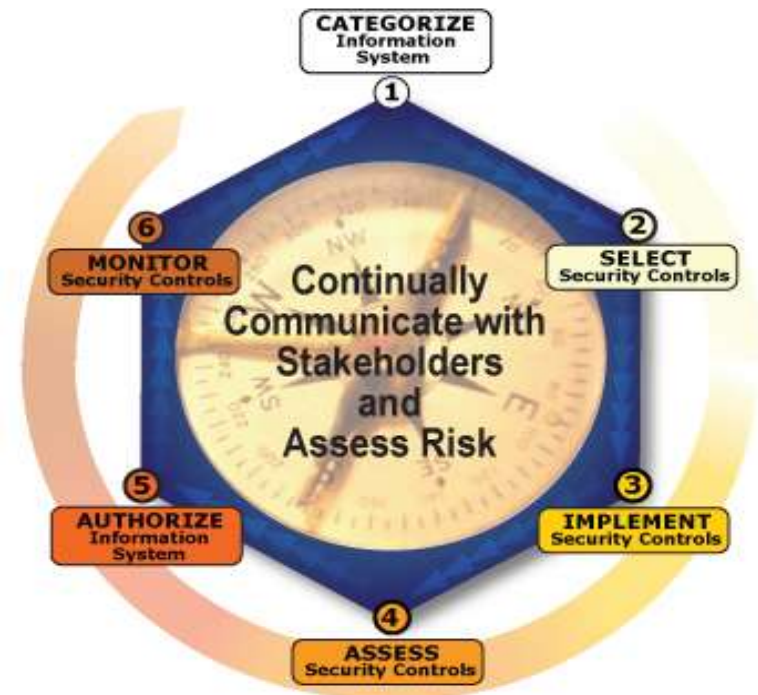


BACKGROUND



Risk Management Framework (RMF)

- **Structured six-step approach to managing risks related to the operation and use of Information Systems (IS)**
- **Framework for certifying and accrediting ISs within the Intelligence Community (IC)**
- **Maintains the security thread throughout the system lifecycle**



Documents

- **Intelligence Community Directive (ICD) 503**
 - Overarching policy on risk management, certification and accreditation
 - Rescinded Director of Central Intelligence Directive (DCID) 6/3
 - Requires policy implementing guidance

- **NIST SP 800-53 provides**
 - Security controls catalog for all federal government systems – including National Security Systems (NSS)
 - Security control selection process
 - Initial guidance on tailoring and supplementing these controls

- **CNSSI 1253 provides guidance for**
 - Categorization of national security information and NSS
 - Additional tailoring and supplementing guidance for NSS
 - Initial control baselines & minimum variable parameters for NSS



Security Controls

- ***Security controls are safeguards or countermeasures put in place to protect a system and its information***
- **Also referred to as *security requirements***
- **Compromise of an organization's information systems can put at risk:**
 - Organizational operations and assets
 - Individuals
 - Other organizations
 - The Nation



Organization of Controls

- **Security Controls are organized into seventeen families**
 - Related by security functionality
 - Designated by a two-character identifier
- **Programmatic controls are listed in a separate appendix**
- **Families are organized into three classes:**
 - **Operational Controls** - Day-to-day mechanisms used to protect operational systems and environments
 - **Technical Controls** - Hardware/Software controls used to provide automated protection of the IT system or application
 - **Management Controls** - Actions taken to manage the development, maintenance and use of the system



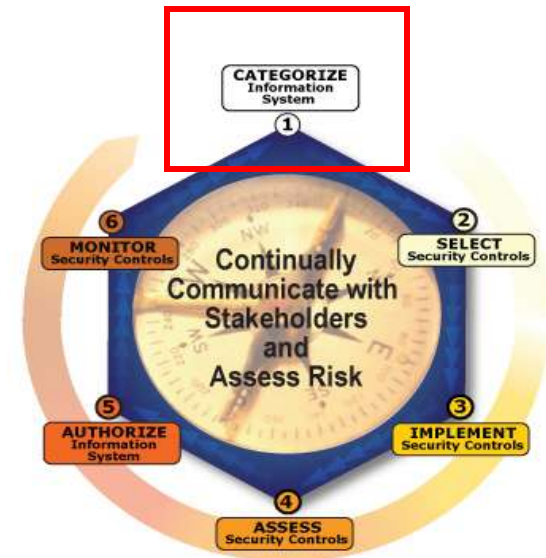


RMF STEP 1 - CATEGORIZE



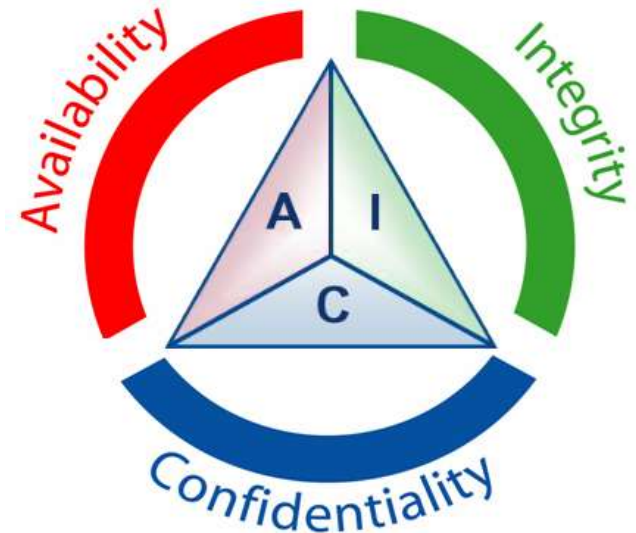
Categorize Overview

- Categorization is a risk-based characterization of information or information systems based on the potential impact of a loss of *confidentiality, integrity, or availability (C-I-A)*
- Three categories of potential impact
 - Low
 - Moderate
 - High
- CNSSI 1253 defines two categorization methodologies for NSS
 - Baseline-based (potential impact)
 - Control Profile-based



Security Objectives: C-I-A

- **There are three security objectives for both information and information systems:**
 - ✓ **Confidentiality (C)**
Information is disclosed only to those authorized to access it
 - ✓ **Integrity (I)**
No unauthorized modification or destruction of information
 - ✓ **Availability (A)**
Information is available when it is needed



Potential Impact

- Security categorization relies on common definitions for each potential impact level

	LOW	MOD	HIGH
Confidentiality Impact: <i>Unauthorized disclosure</i> could have a...	<i>Limited adverse effect</i>	<i>Serious adverse effect</i>	<i>Severe or catastrophic adverse effect</i>
Integrity Impact: <i>Unauthorized modification or destruction</i> could have a...			
Availability Impact: <i>Disruption of access to use</i> could have a...			



Baseline Categorization Method

- **The baseline-based (potential impact) method of security categorization is a three-step process:**

Step 1. Security categorization of information types

Step 2. Security categorization of NSS

Step 3. Risk adjustment of NSS categorization



1. Categorize Information Types

- For each information type on the system, identify the potential impact level (H, M, L) of a breach for each security objective (C, I, A)
- An information type is a specific category of information that is defined by an organization, a law or a policy
- Examples of information types include:
 - Command and Control
 - Personal
 - Administrative
 - Technical Data
 - Proprietary
 - Financial
- An information system may contain more than one type of information

Format for expressing the security category, SC, of an information TYPE is:

SC Info Type = {(Confidentiality IMPACT), (Integrity IMPACT, (Availability IMPACT))}



Example categorization of an information type

SC Info Type = {(Confidentiality HIGH), (Integrity HIGH), (Availability MODERATE)}



2. Categorize the System

- The highest information type impact for each security objective determines the potential impact for the NSS for each objective

Information Type	C	I	A
Information Type A	M	L	L
Information Type B	H	H	M
Information Type C	M	M	M
Information Type D	H	M	L
Highest Information Type Impact	H	H	M

This is the ***National Security System*** impact for each security objective

Format for expressing the security category (SC) of this NSS is:
SC System Name = {(Confidentiality HIGH), (Integrity HIGH), (Availability MODERATE)}



3. Risk Adjustment for categorized system

- Impact level categorization is based on the “worst case” assessment of the potential consequence of a loss of C, I or A
- Organizations may perform a *risk adjustment* of the system’s categorization, based on an assessment of risk and mitigating factors
 - Security afforded by the larger system environment (e.g., physical, personnel, organizational) and its mitigating effect upon external exposure
 - Environmental security measures are typically required to protect classified NSI
- Risk adjustment may result in a change to the system categorization of one or more of the security objectives C, I, or A

Format expressing possible post-risk adjustment for previous example system:

SC *System Name* =

{(Confidentiality HIGH), (Integrity HIGH), (Availability MODERATE)}



SC (Post RA) *System Name* =

{(Confidentiality LOW), (Integrity LOW), (Availability MODERATE)}



Control Profiles Categorization Method

- **Organizations may designate sets of controls for NSS based on an enterprise-wide risk assessment**

- **Security control profiles...**
 - Are pre-defined sets of security controls for specific categories of information
 - Are defined by organizations based on enterprise-wide risk assessment
 - Take into account:
 - business objectives
 - security risks
 - mission needs
 - May be rigidly defined, or loosely defined (*permit tailoring*)



Determining Control Profiles

- **An organization may establish control profiles following a process of its choosing, e.g.:**
 - Organization follows the baseline categorization method to determine the control profile for a specified type of system
 - Organization establishes a set of controls for a specified type of system by mapping NIST SP 800-53 Appendix F controls against a historical framework (such as DCID 6/3 or DoDI 8500.2)
 - Organization evaluates risks and identifies controls to address them

- **The process and rationale for control selection should be described in the system security plan**



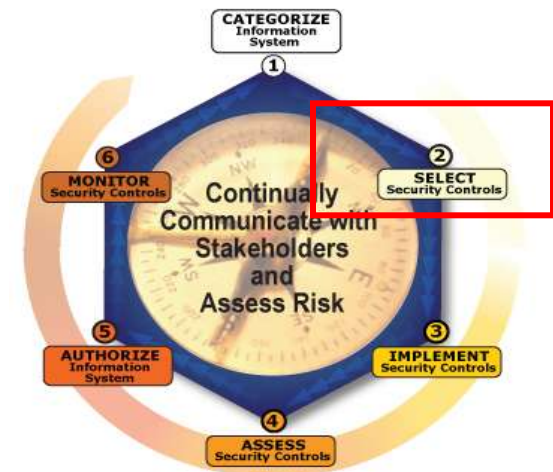


RMF STEP 2 - SELECT



Select Overview

- **Regardless of categorization method, controls are selected from the NIST SP 800-53 control catalog (Appendix F)**
- **The method for selecting controls for both NSS and non-NSS is described in detail in NIST SP 800-53, and is summarized for NSS in CNSSI 1253**
- **CNSSI 1253 provides unique selection guidance for NSS**
 - Additional tailoring, supplementing guidance
 - NSS-unique controls baselines
 - NSS-unique variable instantiations



Control Selection Process

- **Selecting controls is a three-step process*:**

Step 1. Select the initial set of security controls

Step 2. Tailor the initial set of security controls

Step 3. Supplement the tailored set of security controls

****If using the Control Profile Method, refer to the applicable organizational guidance to determine whether tailoring or supplementing of that control profile is permitted or required***



1. Select Initial Set of Security controls*

- **NSS refer to CNSSI 1253 Appendix D for Security Controls Baselines**
- **Identify needed controls from the table based on the system categorization for C, I, A**

Table of Security Controls Baselines (Sample Set)

ID	Title	C			I			A		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy And Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management		X	X		X	X			
AC-2(2)	Account Management		X	X		X	X			
AT-3	Security Training	X	X	X	X	X	X	X	X	X
AT-3(1)	Security Training									
AT-3(2)	Security Training		X	X		X	X		X	X
AU-2(3)	Auditable Events		X	X		X	X			
AU-4	Audit Storage Capacity							X	X	X
AU-5	Response To Audit Processing Failures							X	X	X
AU-5(1)	Response To Audit Processing Failures									X
AU-8	Time Stamps				X	X	X			
AU-8(1)	Time Stamps					X	X			
AU-9	Protection Of Audit Information	X	X	X	X	X	X			

**Step 1 Not applicable for Control Profiles*



2. Tailor the Initial Set of Controls

- **It may be necessary to *tailor* (modify) the initial controls list due to operational considerations**
 - Tailoring decisions must be aligned with operational considerations and the environment of the NSS
 - Controls should not be removed for operational convenience, but have a specified, risk-based determination as established by the system's risk model

- **Three considerations for tailoring:**
 - Scoping guidance
 - Compensating security controls
 - Specification of organization-defined parameters

- **Document tailoring decisions, including the specific rationale for those decisions, in the system security plan**



Tailoring: *Scoping Guidance*

- **Specific terms and conditions on applicability and implementation of individual security controls**
- **Can eliminate unnecessary controls from initial baselines**
- **Takes into account such elements as:**
 - Common Controls
 - Security Objectives
 - System Component Allocation
 - Technology
 - Physical Infrastructure
 - Policy / Regulatory considerations
 - Operational / Environmental considerations
 - Public Access
- ***CNSSI 1253 provides additional scoping guidance for NSS on***
 - *Mobility*
 - *Collaboration and Information Sharing*
 - *System Capabilities / Technology*
 - *Processing & Storage Capability*



A Note on Common Controls

- ***Common Controls are security controls that are inheritable by one or more information systems***
 - E.g., the guard posted in front of a facility protects all of the systems within that facility
 - Other examples might include: contingency planning; incident response planning; security training and awareness; physical and personnel security; common hardware, software, or firmware

- **Organization assigns responsibility for common controls and coordinates their implementation, assessment, and approval**
 - Not the responsibility of a single system owner
 - Centrally managing and documenting common controls can save resources across multiple information systems

- **Common controls are implemented with regard to the highest impact level among the inheriting systems**



Tailoring: *Compensating Controls*

- *Compensating controls are safeguards or countermeasures employed in lieu of a security control recommended in the baseline that provides a comparable level of protection*
- **When selecting compensating controls, the organization must**
 - Select the compensating control from NIST SP 800-53, or adopt from another source
 - Provide supporting rationale for how it delivers an equivalent security capability and why the related baseline security control could not be employed; and
 - Assess and formally accept the risk associated with employing the compensating control



Additional Compensating Guidance for NSS from *CNSSI 1253*

- **Circumstances may require use of compensating controls:**
 - Selected control is not available for or cannot be applied to given NSS
 - Selected control would impose excessive or unnecessary costs on the organization; or
 - Selected control may have a significantly adverse effect on mission requirements
- **Enterprise-implemented controls**
 - Controls implemented & managed at the enterprise level may affect the responsibility of individual system owners
 - Every control must be fully addressed either by the organization or the NSS owner
- **System capabilities / technology**
 - If automated methods are not technically or financially feasible, non-automated compensating controls may be used instead



Tailoring: *Specify Organization-Defined Parameters*

- **Some controls and control enhancements contain certain parameters (variables) that each organization must define (instantiate) as part of the tailoring process**
- **To support reciprocity, these values have been pre-defined for NSS in Appendix E of CNSSI 1253**
- **The *variable instantiations* in CNSSI 1253 are the minimum standard required for NSS**
 - Systems may go beyond this standard
 - Minimum standard facilitates certification reciprocity across National Security Community



Variable Instantiations for NSS

Examples of instantiated variables for NSS from CNSSI 1253

CONTROL NO. (ENHANCEMENT)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
Access Control			
AC-2 (2)	Account Management	The information system automatically terminates temporary and emergency accounts after <i>[Assignment: organization-defined time period for each type of account]</i>not to exceed 72 hours.
AC-2 (3)	Account Management	The information system automatically disables inactive accounts after <i>[Assignment: organization-defined time period]</i>not to exceed 30 days.
AC-2 (5)	Account Management	The organization: (a.) Requires that users logout when <i>[Assignment: organization defined time-period of expected inactivity and/or description of when to logout]</i> ;	a. not to exceed 30 minutes.



3. Supplement the Tailored Set of Controls

- ***Supplement*** the tailored baseline based on a risk analysis of the system

- **Supplementation addresses residual risks from the tailored baseline**
 - Additional security controls or control enhancements may be needed to address specific threats or vulnerabilities; or
 - Additions may be needed to satisfy public laws, executive orders, directives, policies, standards, or regulations

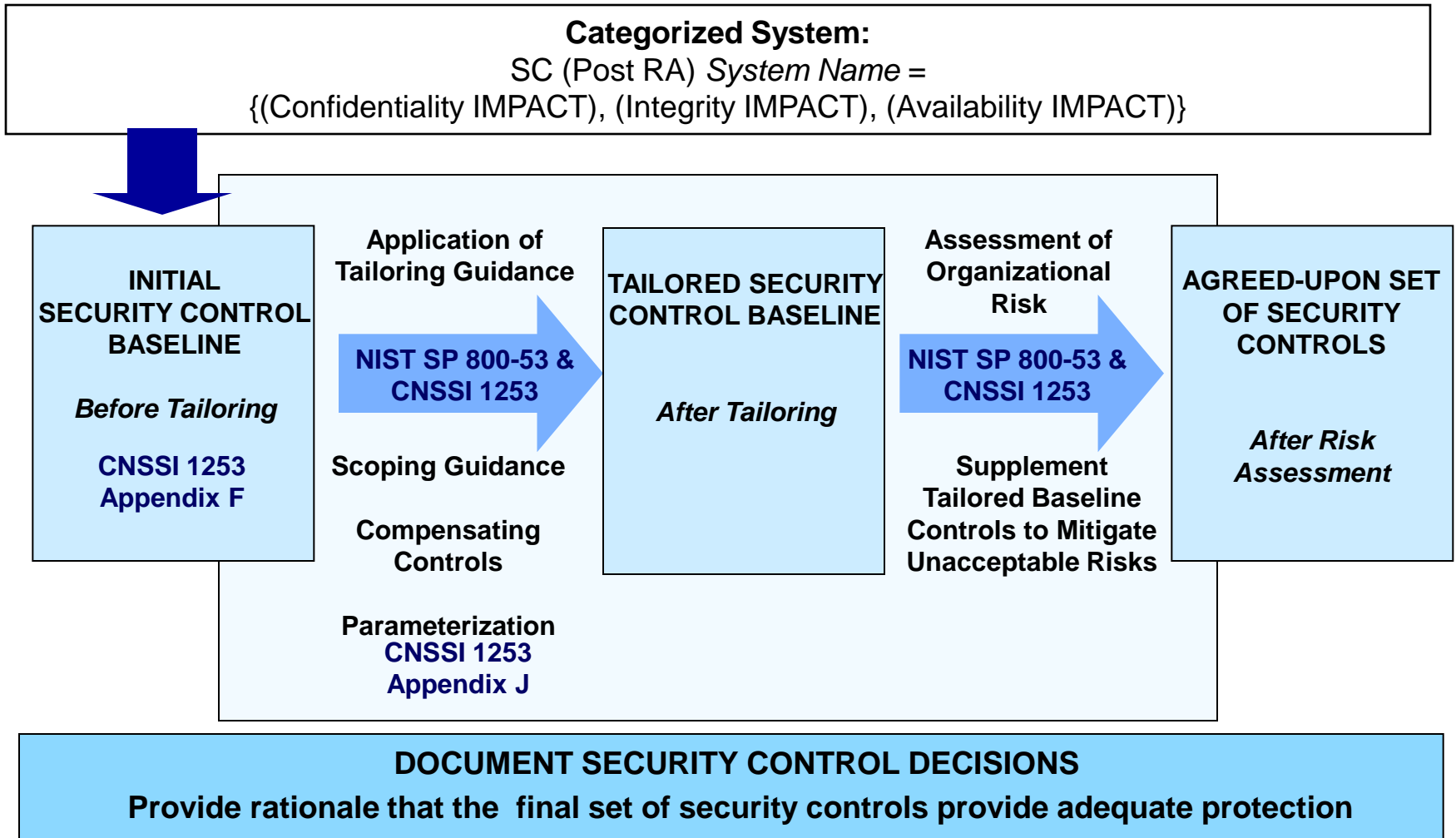


Supplementing: Two Approaches

- **Two approaches to supplementing the tailored baseline:**
 - **Requirements Definition approach** – Begins with specific threat information about certain capabilities or attack potential. Organizations choose additional controls / enhancements from the catalog to effectively withstand such attacks
 - **Gap Analysis approach** – Organization assesses current security capability, then determines the types of threats it can reasonably expect to counter. If current capability is insufficient, the organization chooses additional controls / enhancements from the catalog to achieve desired capability

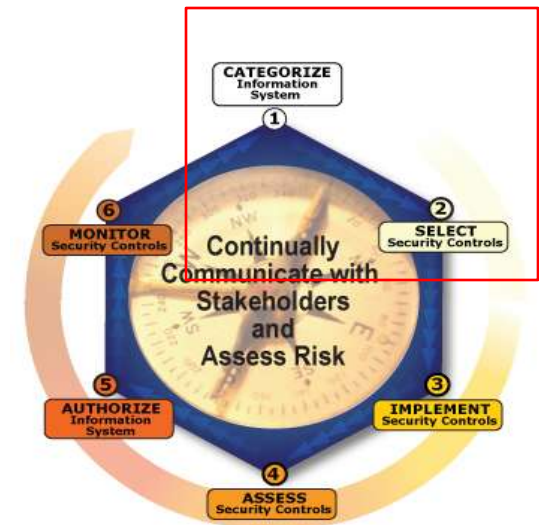


Security Control Selection Process



NIST SP 800-53 and CNSSI 1253

- **For National Security Systems**
 - Follow CNSSI 1253
 - To categorize the system
 - Baseline (Impact) Method
 - Control Profiles Method
 - To select the baseline set of security controls
 - To determine variable instantiations for Assignments
 - Follow NIST SP 800-53
 - For descriptions of all security controls (the controls catalog)
 - For initial guidance on the selection process (tailoring, supplementing)





CONTROLS CATALOG

NIST SP 800-53

“Recommended Security Controls for Federal Information Systems and Organizations”



Security Control Catalog

NIST SP 800-53 Appendix F

- **The catalog lists and describes a range of safeguards and countermeasures for organizations and information systems**

Special Publication 800-53

Recommended Security Controls for Federal Information Systems and Organizations

APPENDIX F

SECURITY CONTROL CATALOG

SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

The catalog of security controls in this appendix provides a range of safeguards and countermeasures for organizations and information systems.⁵³ The organization of the security control catalog, the structure of the controls, and the concept of allocating security controls and control enhancements to the initial baselines in Appendix D are described in Chapter Two. The security controls in the catalog are expected to change over time, as controls are withdrawn, revised and added. In order to maintain stability in security plans and automated tools supporting the implementation of NIST Special Publication 800-53, security controls and control enhancements will not be renumbered each time a control or enhancement is withdrawn. Notations of security controls and controls enhancements that have been withdrawn will be maintained in the catalog for historical purposes.



Control Structure

- **Controls are listed in the catalog alphabetically, by identifier**
- **A number is appended to the family identifier to uniquely identify each control within the family**
- **Each control in the catalog consists of several *sections***
 - Control (description)
 - Supplemental guidance
 - Enhancements
 - References
 - Baseline allocations and sequencing priorities



Listing of Control Identifiers, Families & Classes

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational



Example of a Control Listing

Typical control example from the Auditing and Accountability family

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

- a. Alerts designated organizational officials in the event of an audit processing failure; and
- b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.
Related control: AU-4.

Control Enhancements:

- (1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].
- (2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].
- (3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects or delays*] network traffic above those thresholds.
- (4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

References: None.



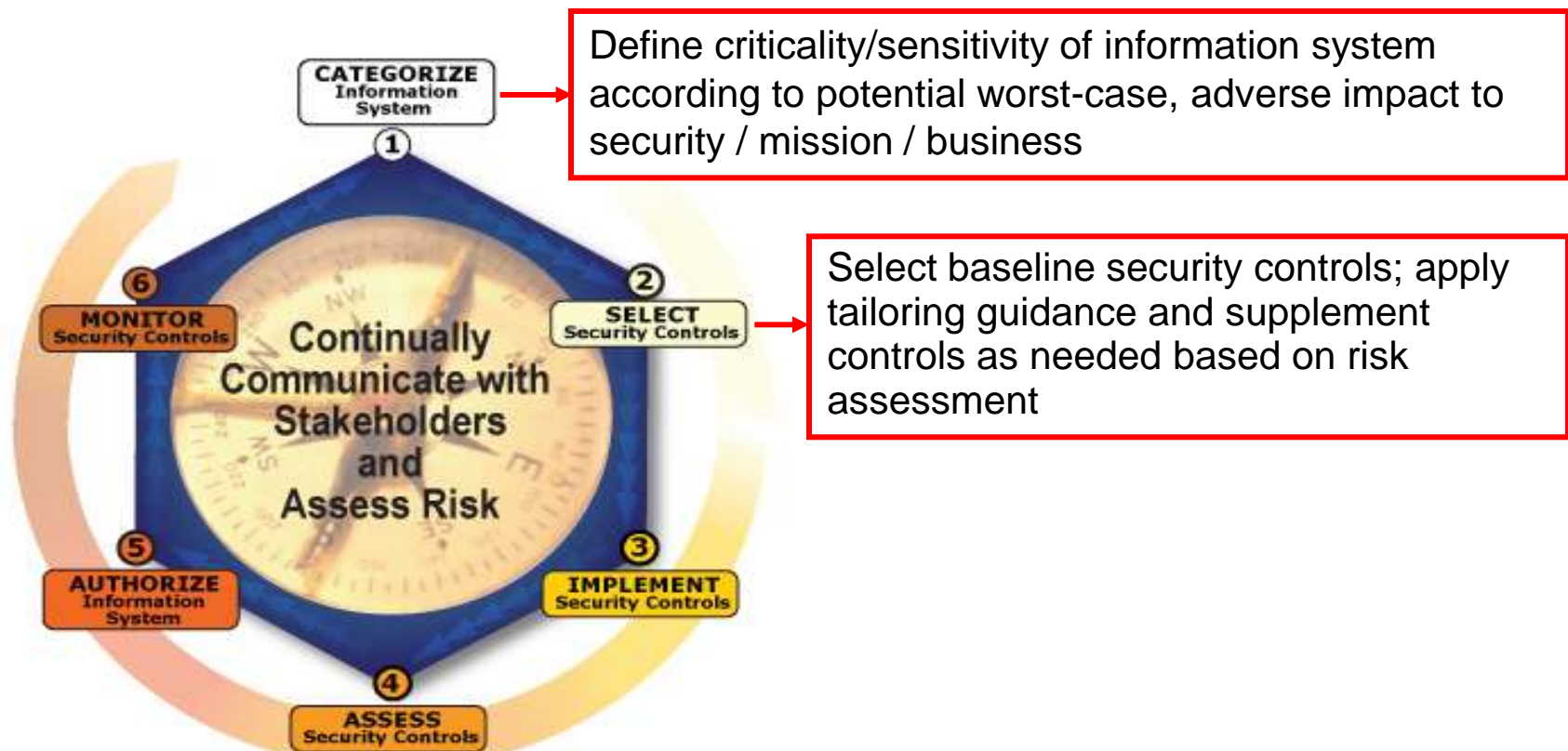


SUMMARY



Categorize and Select

NIST SP 800-53 and CNSSI 1253 are key to performing steps 1 and 2 of the RMF for national security systems



Risk Management Framework



Questions?



Contact Information

- **ODNI CIO C&A Transformation Team:**
 - Roger Caslow, 703-983-3340
roger.caslow@ugov.gov
 - Jennifer Fabius Greene, 703-983-3449
jgreene@mitre.org

- **Websites:**
 - Intelink-U website:
 - <https://www.intelink.gov/ICTG/ca.intel>
 - Intelink-TS website: http://www.intelink.ic.gov/ICTG/ppd_ca.intel

